CLMPTO

10-21-01

MBL

CLAIM 1 CANCELED

CLAIM 2

ADDED

2. (New) A method for establishing a common key k between a central station Z and a group of subscribers T1-Tn, comprising:

providing a publicly known mathematical group G and an element g∈G of a high order in the group G, so that for the group G and the element g a calculation of a discrete logarithm is essentially impossible;

using a predetermined threshold method, wherein a random number i is generated by each subscriber Ti of the group of subscribers T1-Tn, and from the element g∈G and the random number i, the value g^i is calculated by each subscriber Ti of the group of subscribers T1-Tn and transmitted to the central station Z; in the central station Z, a random number z is generated; from the random number z and the values g^i, the values $(g^i)^z$ in the group G are calculated, from the values $(g^i)^z$, n shares $(s_1,\ldots,s_n)$ of the threshold method are derived, and from the shares $(s_1,\ldots,s_n)$, an (n,2n-1) threshold method is constructed, a secret of the (n,2n-1) threshold method being the key k to be established; in the central station Z, n-1 further shares $(s_{n+1},\ldots s_{2n-1})$ differing from shares $(s_1,\ldots,s_n)$ are calculated together with the value g^z in the group G and are transmitted to the group of subscribers T1-Tn; and for each subscriber Ti of the group of subscribers

T1-Tn, the key k to be established is reconstructed so that from the value g^z transmitted by the central station Z and the random number i of each subscriber Ti of the group of subscribers T1-Tn, the value $(g^z)^i$ in the group G is calculated, and that from the resulting value, applying the (n,2n-1) threshold method, the share s_i is derived, and that using the share s_i and the further shares $(s_{n+1},\ldots s_{2n-1})$ transmitted by the central station Z, the key k is reconstructed.